УДК 316.42 + 316.77+008

С. В. Масленченко

АКТУАЛЬНЫЕ ТРЕНДЫ В РАЗВИТИИ КИБЕРПРЕСТУПНОСТИ И ПОТЕНЦИАЛЬНЫЕ МЕХАНИЗМЫ ИХ НЕЙТРАЛИЗАЦИИ

Известная истина о том, что все течет и изменяется, в полной мере может относиться и к сетевому пространству, а также к виртуализированным в нем социальным группам и институтам.

За последние 5 лет проявились две тенденции развития киберреальности: во-первых, происходят новые стратификационные процессы внутри сообществ пользователей; во-вторых, меняется динамика преступной активности в сетевом пространстве.

Хакеры, которые в конце 1990-х годах представляли собой аморфную общность, в 2000-х годах разделились на «белых» (преимущественно осуществляющих правомерную, как правило, коммерческую деятельность по поиску уязвимостей в IT-безопасности компаний и информационном продукте) и «черных» (кракеров) хакеров, объективирующих преступную деятельность.

Технологическое развитие последних лет позволило кракерам интенсифицировать свою противоправную активность и привело к формированию следующих трендов:

1. Постоянно растет средняя мощность DDoS-атаки и сокращается ее продолжительность. Например, в Рунете в 2012 году средняя скорость DDoS-атаки составляла 34 Мб/с при продолжительности в 11 часов 19 минут; в 2013 году – 5,5 Гб/с и 4 часов 57 минут; в 2014 году – пиковая скорость атак возросла до 60–120 Гб/с.

2. Атаки все чаще носят комбинированный характер. Как правило, DDoS-атаки сопровождаются другими видами хакинга. По данным компании Group-IB, доход злоумышленников, организующих DDoS-атаки, в России в 2012 году снизился на 15,4 % – до 110 миллионов долларов по сравнению с 130 миллионами долларов в 2011 году.

3. Наиболее частые объекты интернет-атак – ресурсы интернет-торговля и СМИ. Только в 2012 году около 25 % всех DDoS-атак в России были направлены на отрасль интернет-торговли, около 20 % – на средства массовой информации, в то время как на ресурсы государственных органов власти – 8 %, по на игровые сайты и банковские структуры по – 15 %, на прочие интернет-объекты – около 17 %. «Основными целями злоумышленников, практикующих DDoS-атаки, являются приостановка коммерческой деятельности компании, кража данных, вымогательство и лишение конкурентных преимуществ и репутации организации».

4. Рост ущерба. Согласно совместному докладу НАИРИТ и Института системного анализа РАН и Института социально-экономической модернизации, «общий объем потерь российской экономики от попыток незаконного электронного вмешательства за 2013 год превысил 1,3 триллиона рублей».

Исследование данных трендов выявило полное отсутствие отечественной статистики, что вновь делает актуальным вопрос о необходимости сбора и анализа подобной информации с целью выработки мер по минимизации потенциальных негативных последствий. Данные, приводимые по российскому сегменту интернет-пространства, обладают определенной репрезентативностью, поскольку демонстрируют аналогичные с Байнетом тенденции развития.

Для организации подобного рода атак требуется не более 5 минут активации ботов и 200 USD, при этом средний доход кракера за один «парализованный» ресурс – 100 USD в сутки.

Практикуемым способом нейтрализации DDoS-атак становится простое отключение ресурсов, на которые они направлены, в целях защиты иных объектов и серверных возможностей провайдера-поставщика услуг.

При реализации данных предложений целесообразно учитывать уже накопленный мировой опыт. В странах с развитой информационной и сетевой структурой стало традиционным проведение следующих мероприятий, призванных повысить информационную и технологическую защищенность в киберпространстве:

во-первых, реализация программ по повышению информационной грамотности среди сотрудников и персонала, так называемых «критических» объектов, к которым относят государственные и коммерческие структуры, чья деятельность носит системоообразующий характер и ее дезорганизация наносит вред национальной безопасности (например, крупнейшие в мире учения «Недремлющая акула II» (Waking shark II), в ходе которых симулируется кибератака на банки и финансовые учреждения для проверки существующих систем безопасности и механизмов координации действий между заинтересованными организациями (Bank of England, Barclays, BNP, Bank of America, Deutsche Bank, JP Morgan, Goldman Sachs и др.);

во-вторых, реализация задач по импортозамещению техники, технологий и программного обеспечения информационно-коммуникативной отрасли с целью недопущения активизации встроенного вредоносного программного обеспечения и удаленного доступа к управлению стратегически важными объектами.

В целях преодоления негативных последствий возрастающей преступной киберактивности необходимо осуществление государством ряда управленческих и профилактических мероприятий:

1. Создание государственной структуры, которая бы отвечала за кибербезопасность в двух сферах: защита от внешних киберугроз (аналог Киберкомандования США) и защита от внутренних киберугроз (киберполи-

ция/кибермилиция). В случаях осуществления преступной деятельности из-за территориальных пределов страны или шпионской деятельности внутри страны подобного рода ведомство оперативно решало бы вопросы противодействия, минуя многочисленные межведомственные процедуры согласования.

2. Организация подготовки специализированных кадров по противодействию киберугрозам (как военного, так и криминального характера) и повышения их квалификации.

УДК 343.622 (621)

Ю. Ф. Машталер

ОТГРАНИЧЕНИЕ ПОСЯГАТЕЛЬСТВА НА ЖИЗНЬ НОВОРОЖДЕННОГО РЕБЕНКА ОТ НЕЗАКОННОГО ПРОИЗВОДСТВА АБОРТА

Реализация государственной программы заботы о воспроизводстве подрастающего поколения, его воспитании и развитии предполагает защиту как плода, так и жизни ребенка с момента рождения. Так, в п. 3 ч. 2 ст. 139 Уголовного кодекса Республики Беларусь (далее – УК) предусмотрено в качестве одного из квалифицирующих обстоятельств (признаков) преступлений против жизни – убийство заведомо для виновного беременной женщины, а в п. 2 ч. 2 ст. 139 УК указаны в качестве квалифицирующих признаков посягательств на жизнь детей – убийства заведомо малолетнего, престарелого или лица, находящегося в беспомощном состоянии.

Если в судебно-следственной практике при квалификации посягательств в отношении женщин, находящихся в состоянии беременности, с учетом разъяснений постановления Пленума Верховного Суда Республики Беларусь № 9 от 17 декабря 2002 г. затруднений не возникает, то в отношении применения п. 2 ч. 2 ст. 139 УК этого сказать нельзя. В названном постановлении Верховным судом разъяснено, что под «беспомощным следует понимать такое состояния оказывать преступнику активное сопротивление, уклоняться от посягательства или иным образом ему препятствовать. К лицам, находящимся в беспомощном состоянии, можно отнести, в частности, тяжелобольных либо страдающих психическими расстройствами, лишающими их способности правильно воспринимать происходящее». При этом, квалифицируя убийство ребенка по признаку малолетнего возраста, не исключается квалификация и по признаку беспомощного состояния.

При убийстве матерью, отцом или иным лицом своего или чужого ребенка в возрасте от момента рождения до 14 лет содеянное должно квалифициро-